

105(12/24/2005) Cam 12/27/2005

DEC 29 2005

PTO/SB/08a (08-03)

Approved for use through 07/31/2008. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

# **INFORMATION DISCLOSURE STATEMENT BY APPLICANT**

(use as many sheets as necessary)

Sheet 1 of 2

## **Complete if Known**

Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Justin T. Darrow
Attorney Docket No.r	44424162-8724

## **OTHER ITEMS - NON PATENT LITERATURE DOCUMENTS**

Examine r Initials*	Cite No.†	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T‡
BO		Posting on sci.crypt newsgroup, RIVEST, Ron, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-11-95, retrieved from internet 11-19-05, <a href="http://groups.google.com/group/sci.crypt/msg/79e75dc930adf7dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/79e75dc930adf7dmode=source&amp;hl=en</a> .	
BO		Posting on sci.crypt newsgroup, KOCHER, Paul C, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-11-95, retrieved from internet 11-19-05, <a href="http://groups.google.com/group/sci.crypt/msg/027dadba758893a5?dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/027dadba758893a5?dmode=source&amp;hl=en</a> .	
BO		Posting on sci.crypt newsgroup, WALTERS, Jim, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-11-95, retrieved from internet 11-19-05, <a href="http://groups.google.com/group/sci.crypt/msg/77b761989c18baca?dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/77b761989c18baca?dmode=source&amp;hl=en</a> .	
BO		Posting on sci.crypt newsgroup, KOCHER, Paul C, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-12-95, retrieved from internet 11-22-05, <a href="http://groups.google.com/group/sci.crypt/msg/769112d9a7a17488?dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/769112d9a7a17488?dmode=source&amp;hl=en</a> .	
BO		Posting on sci.crypt newsgroup, RUBIN, Paul, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-12-95, retrieved from internet 11-22-05, <a href="http://groups.google.com/group/sci.crypt/msg/7c8fva520b1b5482?dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/7c8fva520b1b5482?dmode=source&amp;hl=en</a> .	
BO		Posting on sci.crypt newsgroup, BROWN, Ralf, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-12-95, retrieved from internet 11-22-05, <a href="http://groups.google.com/group/sci.crypt/msg/417b42c49fe7cf53?dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/417b42c49fe7cf53?dmode=source&amp;hl=en</a> .	
BO		Posting on sci.crypt newsgroup, STEWART, Bill, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-13-95, retrieved from internet 11-22-05, <a href="http://groups.google.com/group/sci.crypt/msg/7610aca60249ed48?dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/7610aca60249ed48?dmode=source&amp;hl=en</a> .	
BO		Posting on sci.crypt newsgroup, Larry, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-15-95, retrieved from internet 11-22-05, <a href="http://groups.google.com/group/sci.crypt/msg/ced8289a35a32925?dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/ced8289a35a32925?dmode=source&amp;hl=en</a> .	
BO		Posting on sci.crypt newsgroup, COSTA, Bob, "Re: Attacking machines on the Internet (re: Timing cryptanalysis of RSA, DH, DSS)", 12-16-95, retrieved from internet 11-22-05, <a href="http://groups.google.com/group/sci.crypt/msg/350820497cce62ba?dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/350820497cce62ba?dmode=source&amp;hl=en</a> .	
Examiner Signature	Justin Darrow		Date Considered 04/30/2006

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. † Applicant's unique citation designation number (optional). ‡ See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. § Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). ¶ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. \*\* Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. \* Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Substitute for form 1449B/PTO				<b>Complete if Known</b>	
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (use as many sheets as necessary)				Application Number	09/930,836
				Filing Date	August 15, 2001
				First Named Inventor	Paul C. Kocher
				Group Art Unit	2132
				Examiner Name	Justin T. Darrow
Sheet	2	of	2	Attorney Docket No.	44424162-8724
<b>OTHER ITEMS - NON PATENT LITERATURE DOCUMENTS</b>					
Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.			T <sup>2</sup>
JP		Posting on sci.crypt newsgroup, PERRY, Tom, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-17-95, retrieved from internet 11-22-05, <a href="http://groups.google.com/group/sci.crypt/msg/20e43912653f9bd0?dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/20e43912653f9bd0?dmode=source&amp;hl=en</a> .			
JP		Posting on sci.crypt newsgroup, BELL, Jim, "Spread-Spectrum computer clock?", 12-24-95, retrieved from internet 11-22-05, <a href="http://groups.google.com/group/sci.crypt/msg/485abca33cc29703?dmode=source&amp;hl=en">http://groups.google.com/group/sci.crypt/msg/485abca33cc29703?dmode=source&amp;hl=en</a> .			
JP		Posting on mail.cypherpunks, BRANDT, Eli, "Re: Timing Attacks", 12-11-95, retrieved from internet 12-7-05, <a href="http://groups.google.com/group/mail.cypherpunks/msg/fa276adeb23f2b83?dmode=source">http://groups.google.com/group/mail.cypherpunks/msg/fa276adeb23f2b83?dmode=source</a>			
JP		Posting on mail.cypherpunks, Armadillo Remailer, "Re: Timing Attacks", 12-13-95, retrieved from internet 11-22-05, <a href="http://groups.google.com/group/mail.cypherpunks/msg/fedb10d2bcf3ff6f?dmod...">http://groups.google.com/group/mail.cypherpunks/msg/fedb10d2bcf3ff6f?dmod...</a>			
JP		Posting on mail.cypherpunks, HOSELTON, Rick, "Re: Timing Cryptanalysis Attack", 12-14-95, retrieved from internet 11-22-05, <a href="http://groups.google.com/group/mail.cypherpunks/msg/470f2482c69f3212?dmo...">http://groups.google.com/group/mail.cypherpunks/msg/470f2482c69f3212?dmo...</a>			
JP		Declaration of Paul Kocher concerning the 1995 postings, KOCHER, Paul, 12-16-05			
Examiner Signature				Date Considered	
Justin Darrow				04/30/2006	

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.